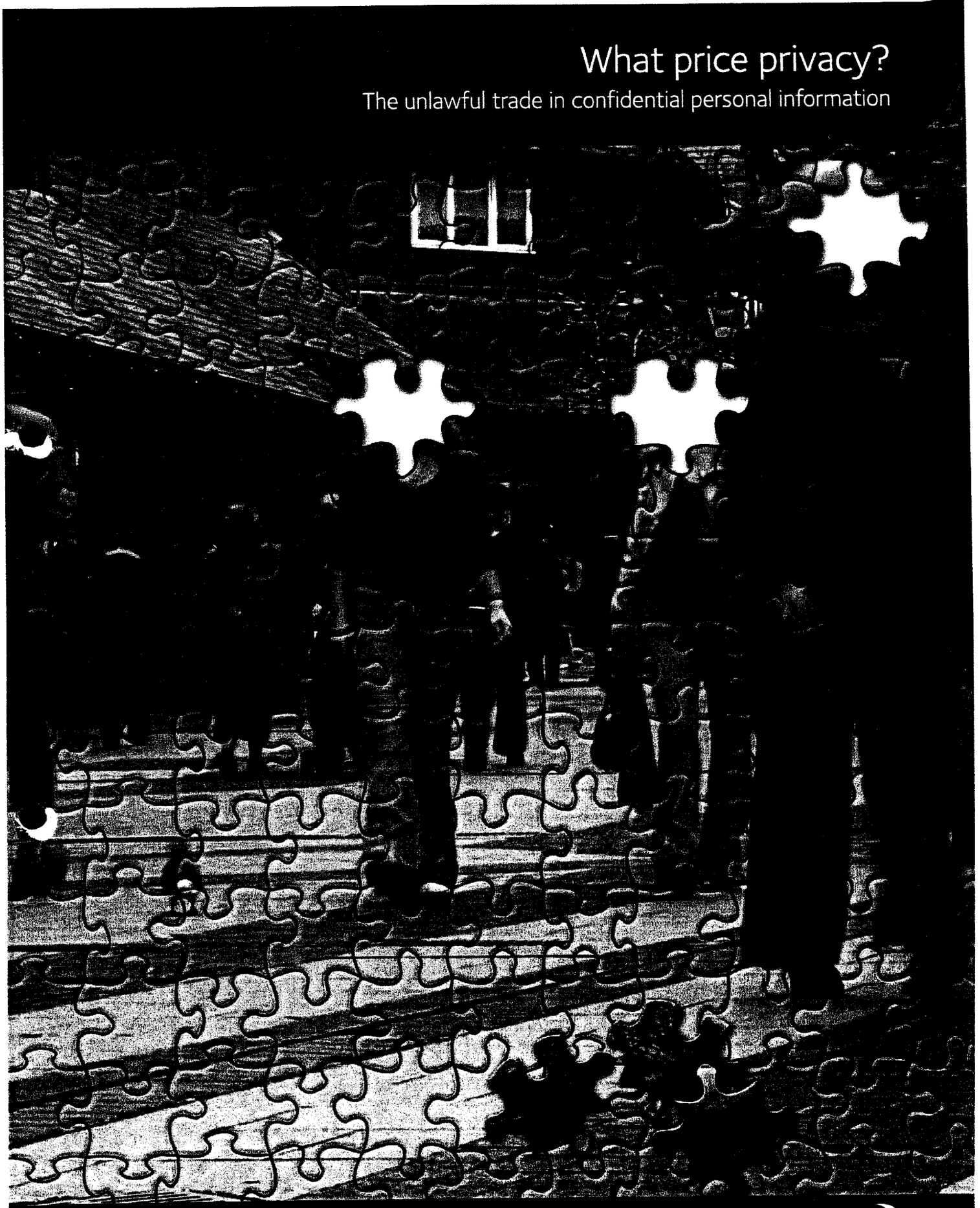
Information Commissioner's Office

What price privacy?

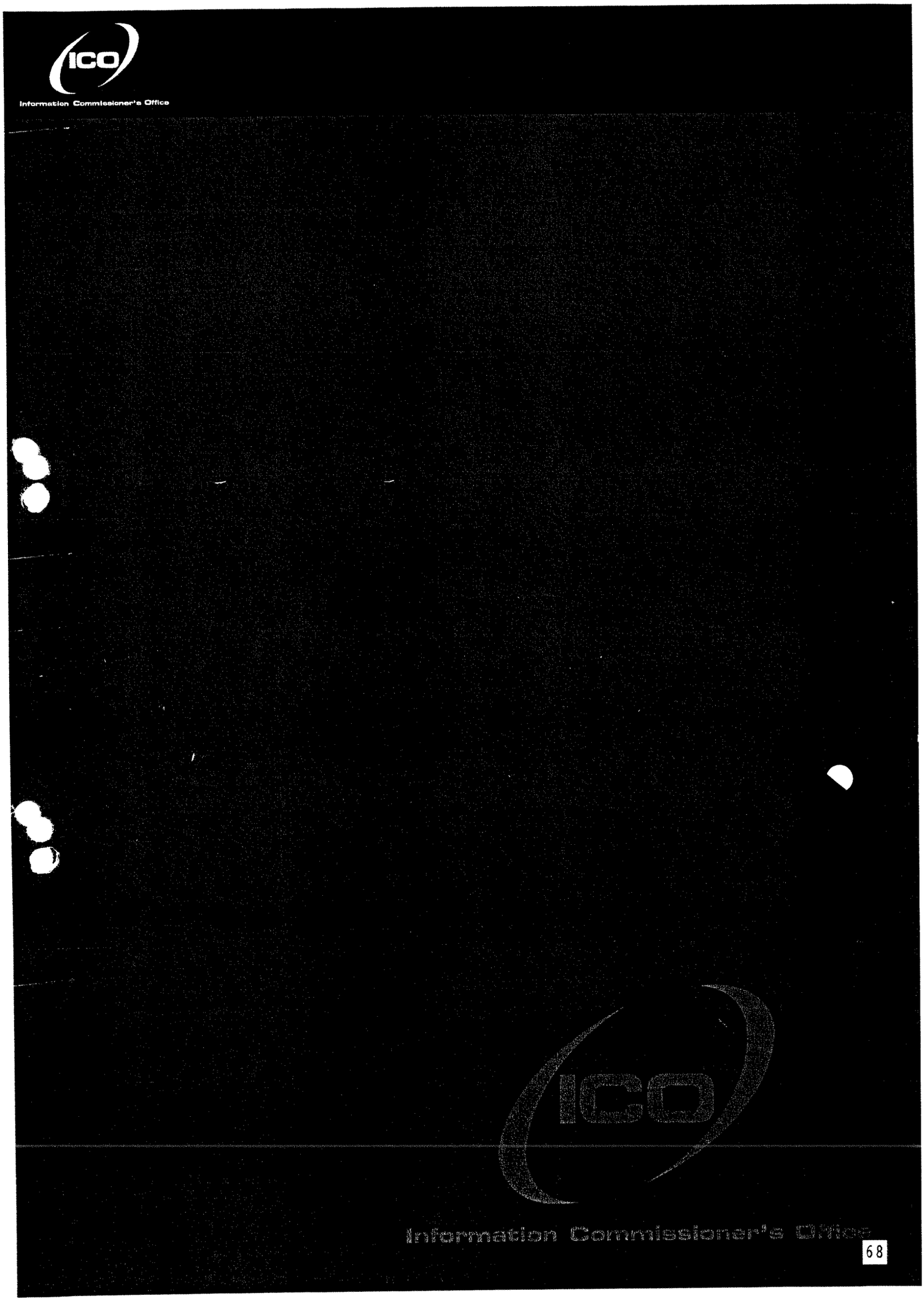
The unlawful trade in confidential personal information



Promoting public access to official information
and protecting your personal information

ICO

Information Commissioner's 67


Information Commissioner's Office
Information Commissioner's Office
68

What price privacy?
The unlawful trade in confidential personal information

Presented by the Information Commissioner to Parliament
pursuant to Section 52(2) of the Data Protection Act 1998

Ordered by the House of Commons to be printed 10 May 2006

London: The Stationery Office

Price: £13.50

HC 1056

Contents

Foreword from The Information Commissioner

Protecting the privacy of the individual goes to the heart of my responsibilities under data protection legislation. Section 55 of the Data Protection Act 1998 makes it an offence to obtain, disclose or 'procure the disclosure' of confidential personal information 'knowingly or recklessly', without the consent of the organisation holding the data. Yet investigations by my officers and by the police have uncovered evidence of a pervasive and widespread 'industry' devoted to the illegal buying and selling of such information.

Personal information has a value – whether it is the embarrassing secret of a celebrity, a politician or someone else in the public eye, or the whereabouts of a private individual who it is thought owes some money. All cases in this illegal trade share in common that they involve personal and private information, and that the organisation holding the information has not authorised its disclosure. Usually stored on computer, these are the jigsaw pieces which help to build up a picture of each one of us as a unique individual. The trade in such information represents so serious a threat to individual privacy that this is the first report I or any of my predecessors have presented to Parliament under the Act's special powers.

The crime at present carries no custodial sentence. When cases involving the unlawful procurement or sale of confidential personal information come before the courts, convictions often bring no more than a derisory fine or a conditional discharge. Low penalties devalue the data protection offence in the public mind and mask the true seriousness of the crime, even within the judicial system. They likewise do little to deter those who seek to buy or supply confidential information that should rightly remain private. The remedy I am proposing is to introduce a custodial sentence of up to two years for persons convicted on indictment, and up to six months for summary convictions. The aim is not to send more people to prison but to discourage all who might be tempted to engage in this unlawful trade, whether as buyers or suppliers.

Individuals are not the only ones who suffer when third parties gain unlawful access to their personal details. Companies risk losing the trust of their customers and confidence in the public sector is shaken. We cannot sensibly build an information society unless its foundations and its systems are secure. Plugging the gaps becomes ever more urgent as the government rolls out its programme of joined-up public services and joined-up computer systems under the banner of transformational government. However laudable the aim, we need to make sure that increasing access to government-held information for those with a legitimate need to know does not also open the door to those who seek to buy, beguile or barter their way to information that is rightly denied to them in law.

These concerns, and the need for increased penalties, have been raised with the Department for Constitutional Affairs. The positive response that I have received so far is encouraging. These are early and welcome indications of progress on the possibility of Government action.

Richard Thomas

Richard Thomas
Information Commissioner

1 Executive Summary

1.1 People care about their personal privacy and have a right to expect that their personal details are and should remain confidential. Who they are, where they live, who their friends and family are, how they run their lives: these are all private matters. Individuals may divulge such information to others, but unless the law compels them to do so the choice is theirs.

1.2 This report reveals evidence of systematic breaches in personal privacy that amount to an unlawful trade in confidential personal information. Putting a stop to this trade is its primary purpose. It is addressed to both Houses of Parliament under the Information Commissioner's powers to lay before them reports of special interest, relating to his functions.[1]

1.3 Public bodies holding personal information about individuals include government departments and agencies, local authorities, the National Health Service and the police. In the private sector, banks and other financial institutions, supermarkets, telephone companies and transport operators may all hold increasing amounts of information about individuals.

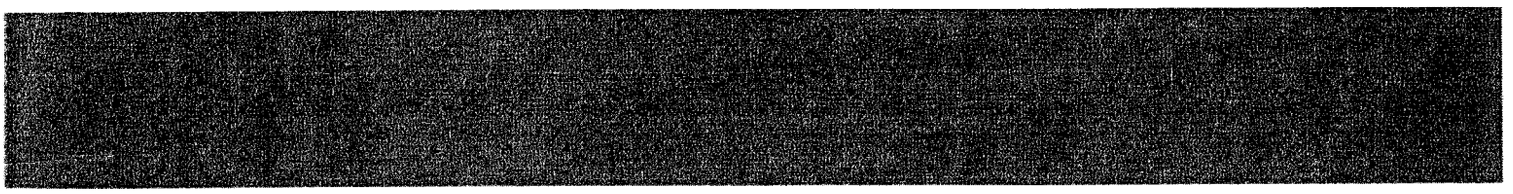
1.4 Government initiatives look set to increase the amount of information collected and shared centrally, and to make it easier for individuals to gain access to their personal details. Such moves inevitably increase the risk of security breaches by third parties.

1.5 Protection is offered in law by section 55 of the Data Protection Act 1998, which makes it an offence (with certain exemptions) to obtain, disclose or procure the disclosure of personal information knowingly or recklessly, without the consent of the organisation holding the information. Offences are punishable by a fine only: up to £5,000 in a Magistrates' Court and unlimited in the Crown Court.

1.6 Since the Act came into force, the Information Commissioner's Office (ICO) has received a steady number of complaints from individuals who feel their privacy has been breached. Many more cases come to the attention of the ICO through joint working protocols with bodies such as the Department for Work and Pensions (DWP), HM Revenue & Customs (HMRC) and police forces around the country.

1.7 Much more illegal activity lies hidden under the surface. Investigations by the ICO and the police have uncovered evidence of a widespread and organised undercover market in confidential personal information. Such evidence forms the core of this report, providing details about how the unlawful trade in personal information operates: who the buyers are, what information they are seeking, how that information is obtained for them, and how much it costs.

1 These powers are contained in the Data Protection Act 1998, Section 52 (2).



1.8 Among the 'buyers' are many journalists looking for a story. In one major case investigated by the ICO, the evidence included records of information supplied to 305 named journalists working for a range of newspapers. Other cases have involved finance companies and local authorities wishing to trace debtors; estranged couples seeking details of their partner's whereabouts or finances; and criminals intent on fraud or witness or juror intimidation.

1.9 The personal information they are seeking may include someone's current address, details of car ownership, an ex-directory telephone number or records of calls made, bank account details or intimate health records. Disclosure of even apparently innocuous personal information – such as an address – can be highly damaging in some circumstances, and in virtually all cases individuals experience distress when their privacy is breached without their consent.

1.10 The 'suppliers' almost invariably work within the private investigation industry: private investigators, tracing agents, and their operatives, often working loosely in chains that may include several intermediaries between ultimate customer and the person who actually obtains the information.

1.11 Suppliers use two main methods to obtain the information they want: through corruption, or more usually by some form of deception, generally known as 'blagging'. Blaggers pretend to be someone they are not in order to wheedle out the information they are seeking. They are prepared to make several telephone calls to get it. Each call they make takes them a little bit further towards their goal: obtaining information illegally which they then sell for a specified price. Records seized under search warrants show that many private investigators and tracing agents are making a lucrative profit from this trade.

1.12 Prosecutions brought under the Act have generally resulted in low penalties: either minimal fines or conditional discharges. Between November 2002 and January 2006, only two out of 22 cases produced total fines amounting to more than £5,000. Other investigations led to frustrating outcomes, despite the detriment caused to individuals and to public confidence generally.

1.13 In the report's central recommendation, **the Information Commissioner calls on the Lord Chancellor to bring forward proposals to raise the penalty for persons convicted on indictment of section 55 offences to a maximum two years' imprisonment, or a fine, or both; and for summary convictions, to a maximum six months' imprisonment, or a fine, or both (paragraph 7.8)**. The aim is to discourage this undercover market and to send out a clear signal that obtaining personal information unlawfully is a serious crime.

1.14 To stifle demand for confidential personal information, **the Information Commissioner further issues a warning to all businesses and individuals obtaining, supplying or buying personal information, that they should restrict themselves to information which they are confident has been lawfully obtained (7.11).**

1.15 The Information Commissioner then addresses these recommendations to some of the main players:

- **The Security Industry Authority should include a caution or conviction for a section 55 offence among the grounds for refusing or revoking the licence of a private investigator (7.14).**
- **The Association of British Investigators should extend its National Occupational Standard for Investigation to include explicit reference to section 55 offences, and undertake other specific measures aimed at raising standards among private investigators (7.16).**
- **The Press Complaints Commission should take a much stronger line to tackle press involvement in this illegal trade (7.21). Furthermore, the Information Commissioner will not hesitate to prosecute journalists identified in previous investigations who continue to commit these offences (7.22).**

1.16 **The Information Commissioner supports efforts to develop legitimate means for tracing genuine debtors. But he calls on the Office of Fair Trading to amend its 2003 Debt Collection Guidance - which is directly linked to fitness to hold a consumer credit licence - to condemn section 55 offences (7.25 and 7.26).**

1.17 To help raise awareness and to encourage good practice, **the Information Commissioner will continue discussions with all the parties involved (7.29). In particular, the Commissioner invites a number of named media, financial and professional bodies to respond to specific questions about the steps they will take to achieve this (7.30, 7.32). The Information Commissioner also invites responses and further evidence from consumer and citizens' organisations (7.33).**

1.18 **As a next step, the Information Commissioner intends to publish a follow-up report 6 months after the publication of the report, documenting responses and progress (7.35).**

2 The context: the data-based society

Who holds confidential information?

2.1 Almost every organisation we deal with in our daily lives holds some personal information about us. Much of this information will be confidential. It will be information that we do not want other people to have unless we say they can have it. Some personal information is especially sensitive, such as details about our sexual lives, our health, or any previous criminal convictions.[2] Information of this nature, if disclosed, could cause upset, embarrassment, hurt, or worse. But the unsanctioned release of even non-sensitive information can of itself cause considerable distress.

2.2 The public bodies holding confidential personal information about an individual include the Department for Work and Pensions (DWP), HM Revenue & Customs (HMRC), local authorities, the Passport Office, the Driver and Vehicle Licensing Authority (DVLA), NHS trusts and medical practitioners, schools and education authorities. Accessible within seconds through more than 10,000 terminals across the country, the Police National Computer (PNC) holds extensive information on criminals, arrested suspects, vehicles and property.

2.3 In the private sector, our details will be recorded by utility and telecommunications companies, banks and other financial institutions, and credit reference agencies. The growth in supermarket loyalty cards has led to the creation of extensive databases containing details of our spending and shopping habits. Transport operators using smart-card technology will also store detailed information about an individual's travel patterns. Not only do more and more bodies hold our basic personal details in their systems, but new information may be added every day. According to one estimate, information about the average working adult is stored on some 700 databases.[3] In both public and private sectors, much of the personal information stored about individuals is accessible via call centres, drawing on information held electronically and sometimes manually.

2.4 The trend towards accumulating more information about people – and creating a detailed picture of an individual's activity – is well illustrated in the field of telecommunications. On 21 February 2006, the Council of the European Union approved the data retention directive, amending the existing directive on privacy and electronic communications (2002/58/EC). The new directive will require providers of telephone, text and internet communications to retain data on traffic (calls made and received) and location (detailing the point where a call is made) but not the content of any communications, for a minimum of 6 months and a maximum of 24 months. Some UK providers currently store these data for up to 12 months under a voluntary code of practice.

2 Section 2 of the Data Protection Act 1998 defines sensitive personal data as relating to a person's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of any offences, and court proceedings.

3 See Lisa Kelly, 'Data protection – who's watching you?', Accountancy Age, 20 August 2004, online edition.

2.5 As a counterbalancing force, the principles of data protection set out in law require that personal information shall be 'adequate, relevant and not excessive' and also that it shall not be kept for longer than is necessary.[4] Minimising the amount of personal information kept and processed by all these organisations is part of the Information Commissioner's brief.

A joined-up future

2.6 As official databases grow in size, there is a corresponding move to join up all the separate holdings, sharing information and allowing a single point of entry into the system. Much of the thrust is government-inspired, most recently in the Cabinet Office's report on transformational government. The strategy aims to give citizens, customers and businesses simple access to services, with a choice of consistent entry points and with seamless handovers between channels such as telephone and internet.[5] Noting the existence of at least 130 major call centres within central government alone, the report goes on to promise their rationalisation, building on work already done by the National Audit Office and many local authorities.

2.7 The new Department of Health agency, NHS Connecting for Health, is bringing modern computer systems into the National Health Service in what it describes as 'the world's largest civil IT programme'.[6] Over the next 10 years, the aim is to connect more than 30,000 GP surgeries to almost 300 hospitals, giving patients access to their personal health and care information. Over 90,000 healthcare workers – from GP receptionists to clinical practitioners - are expected to have direct access to the system, set at different levels according to their requirements.

2.8 The proposed introduction of identity cards will also see the creation of a National Identity Register. Schedule 1 of the Identity Cards Act 2006 sets out the information that may be recorded in the register. It includes personal information, identifying information, residential status, personal reference numbers, record history, registration and ID card history, validation and security information, as well as records of when, what and to whom information from the register has been provided.

2.9 The Children Act 2004 gave the Secretary of State power to create a database or series of local databases to include all 11 million children in England, creating a personal electronic file for each child. Proposed originally in response to the Victoria Climbié tragedy and ensuing enquiry, the Children's Register is intended to include name, address, date of birth, school and GP. The system will flag the files of children known to be 'at risk'.

4 Data Protection Act 1998, Schedule 1, The Data Protection Principles, Part 1, (3) and (5).

5 Cabinet Office, Transformational Government Enabled by Technology, Cm 6683, November 2005, p. 9, para. 31.

6 NHS Connecting for Health, Business Plan 2005-2006, www.connectingforhealth.nhs.uk/publications, p. 36.

3 Developing the legal framework

Why privacy matters

3.1 Respect for privacy is one of the foundation stones of the modern democratic state. It was written into the European Convention on Human Rights, which guarantees certain fundamental human rights. Article 8 of the Convention declares that 'Everyone has the right to respect for his private and family life, his home and his correspondence'. Adopted by the Council of Europe in 1950, the Convention is directly enforceable in UK courts through the Human Rights Act 1998.

3.2 Failure to respect an individual's privacy can lead to distress and in certain circumstances can cause that individual real damage, mentally, physically and financially. Furthermore, privacy is in itself a value that needs protecting, even when the loss suffered is not readily quantifiable in terms of damage or distress.

3.3 Regular research conducted for the ICO into public attitudes gives us some idea of the value people place on privacy. In 2005, respondents put 'protecting people's personal information' equal third in their list of social concerns, alongside the National Health Service.[7] Preventing crime and improving standards in education were ranked first and second. But protecting personal information came ahead of other issues of current public concern, including equal rights for everyone, freedom of speech and national security. The surveys also show that public concern about personal privacy is growing. When questioned further about the consequences of mishandled information, people say they worry especially about threats to personal safety and health, and about financial loss.

Framing the offence

3.4 The specific offence of disclosing confidential personal information without consent was not included in the UK's first data protection legislation introduced in 1984. It arose indirectly out of a few well-publicised breaches of personal privacy, including one experienced in November 1992 by the then Chancellor of the Exchequer, the Rt. Hon. Norman Lamont, when a bank employee leaked details of his credit-card spending. This sparked intrusive press interest into purchases he may have made at a London off-licence.[8]

7 Report on the Information Commissioner's Office, Annual track 2005, www.ico.gov.uk/documentUploads/final_report_individuals_6_10_05.pdf, P.8.

8 The story reached international audiences, as reported by Julian Barnes in his column for The New Yorker and reprinted as 'The Chancellor of the Exchequer Buys Some Claret' in Julian Barnes, Letters from London, 1990-95 (London, Picador, 1995), pp. 160-76.

3.5 Concern at the alleged ease in obtaining details about an individual's bank or tax records and other personal information surfaced in the 1993 annual report of the then Data Protection Registrar, Eric Howe, precursor to the Information Commissioner. Although he expressed himself pleased with the response of major financial institutions to his request that they should tighten their security procedures, he mooted the idea of sanctions against those who tried or succeeded to gain unauthorised access to personal information. In a House of Lords debate in March 1994, the government announced its intention to create the specific offence of obtaining unauthorised access to personal data by deception. New clauses (section 5(6) – 5(11)) were duly added to the Data Protection Act 1984 by Section 161 of the Criminal Justice and Public Order Act 1994,[9] and consolidated in later legislation. The amendments were considered important because they created new criminal offences, but no change was made to the penalties which already applied to other provisions in the law.

The Data Protection Act 1998

3.6 The offence of unlawfully obtaining personal information is now covered by section 55(1) of the Data Protection Act 1998. This states that:

'A person must not knowingly or recklessly, without the consent of the data controller –

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data.'[10]

3.7 As the Act further makes clear in section 55(4), 'A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1)'; and advertising the information for sale constitutes an offer to sell it.

3.8 The Act allows certain defences, set out in section 55 (2). For instance, exemptions are permitted where obtaining, disclosing or procuring personal information is considered necessary 'for the purpose of preventing or detecting crime', or was required by legislation or a court order. Exemptions are also allowed for those who act in the reasonable belief they had legal backing, or that they would have obtained permission from the data controller for their actions; and to anyone who shows that obtaining, disclosing or procuring the information was 'in the public interest'.

9 Under this earlier legislation, the Data Protection Registrar (DPR) could take action only if the data user (since redefined as the data controller) was registered with him, and if disclosure was outside the terms of the organisation's register entry with the DPR. For example, if an organisation was allowed to disclose information to 'enquiry agents', any disclosure to an enquiry agent was within the law, even if the actual enquiry agent was not authorised.

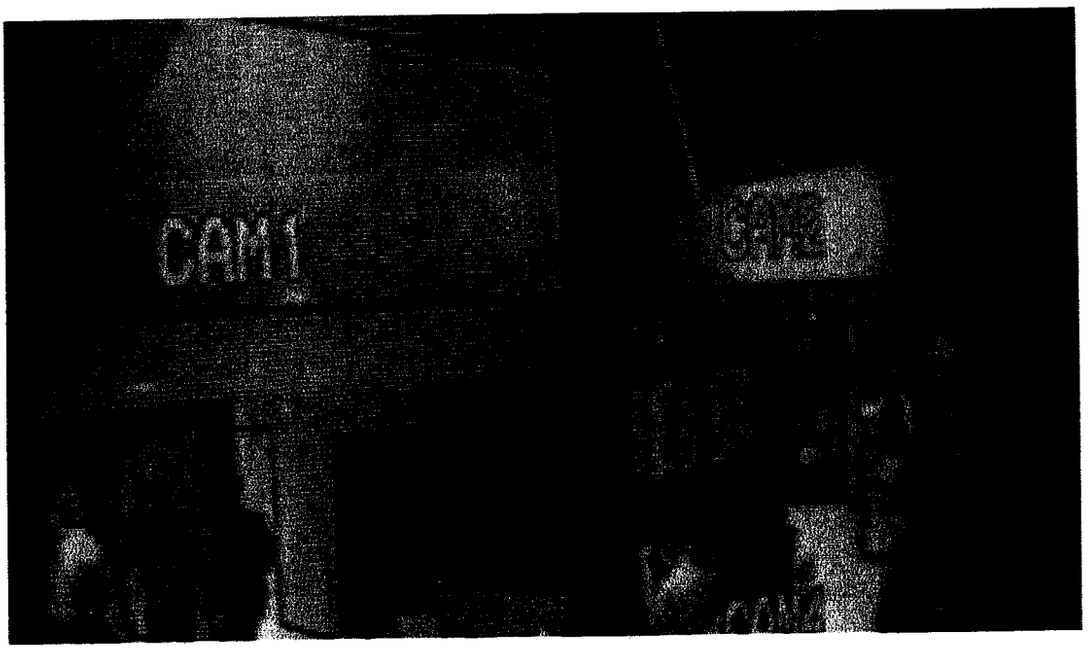
10 For definitions, see paragraph 3.10.

3.9 Section 55 offences may be prosecuted at the instigation of the Information Commissioner or the Director of Public Prosecutions, and tried in either a Magistrates' Court or (in certain circumstances) the Crown Court. They are punishable by a fine only (Section 60(2)). This can be up to £5,000 in a Magistrates' Court (the current maximum for summary convictions) and an unlimited fine for convictions obtained in the Crown Court. The court may also order information connected with the commission of the offence to be forfeited, destroyed or erased.[11] In Scotland, prosecutions are brought by the Procurator Fiscal. The same penalties apply.

Definitions

3.10 As the discussion centres on provisions set out in the Data Protection Act 1998, it is helpful to understand how the Act defines certain terms. By 'data', the Act means information that is recorded or processed electronically by computer, or held manually within a structured filing system. 'Personal data' means data that relate to a living person who can be identified from the information, either separately or together with other bits of information likely to come within an organisation's possession. The organisation holding and processing the information is called the 'data controller', and the individual whose details are held is known as the 'data subject'.

3.11 Technically, the law looks on the organisation whose data has been captured (the data controller) as the 'victim' of the crime, rather than the individual whose details have been stolen (the data subject). In terms of the penalties imposed, the law makes no distinction between offences relating to sensitive or other personal data.



11 Data Protection Act 1998, Section 60(4).

4 Intrusions into individual privacy

Complaints and prosecutions under the Act

4.1 The Data Protection Act came into force on 1 March 2000, and in nearly six years of operation, some 1,000 new Section 55 complaints reached the Information Commissioner's Office (ICO) at an average rate of a little over 180 a year.[12] These have generally originated from individuals who believe their privacy to have been breached. Others are passed on by the police and by agencies whose data may have been targeted.

4.2 Section 55 cases are prioritised in line with the ICO's Regulatory Strategy[13] and those which may result in prosecution are investigated. Between mid-November 2002 and January 2006, the Information Commissioner brought 25 prosecutions in Crown and Magistrates' Courts in England and Wales. Convictions were obtained in all but three cases (of these, two were withdrawn and one discontinued on the orders of the judge). Scotland's Procurator Fiscal brought one successful case to court, and more were prosecuted by the Crown Prosecution Service.

4.3 Details of ICO prosecutions and their outcomes are contained in Appendix A. The statistics are perhaps most revealing for the generally low level of penalties imposed. Out of 22 convictions in England and Wales, one defendant received an absolute discharge and five received conditional discharges ranging from one to two years. Costs awarded against the defendant in these cases ranged from nil to £1,200.

4.4 In a further nine cases, the fine per offence imposed amounted to between £50 and £150, although multiple-offence cases could produce total fines of between £2,000 and £3,000. In the remaining seven cases, the fines ranged from £300 for one offence up to £1,000 per offence in a case involving ten offences, plus a further £5,000 in costs. In only one other case heard during this period did the total fine amount to more than £5,000.

4.5 In September 2000, the Information Commissioner's predecessor joined forces with the Benefits Agency and the Inland Revenue in a concordat known as BAIRD. The aim was actively to investigate people and organisations suspected of systematically and unlawfully obtaining personal information from the two agencies and selling it on to clients. The BAIRD team detected over 100,000 offences, leading to a number of successful prosecutions. Although BAIRD has now concluded, collaboration continues under the new Trident project, launched in November 2004 with agreement between the Information Commissioner, HM Revenue & Customs (HMRC) and the Department

12 Statistics logged since 2002/3 show 183 cases for that year, 185 in 2003/4, 184 in 2004/5 and 109 between April 2005 and January 2006.

13 A strategy for data protection regulatory action. Information Commissioner's Office, 2005. www.ico.gov.uk/DocumentUploads/Data_Protection_Regulatory_Action_Strategy.pdf

for Work and Pensions (DWP) to conduct proactive investigations into section 55 offences. Whenever HMRC or DWP staff identify suspect calls, they complete a bogus call report. These reports are collated and analysed, and when patterns are identified the cases are passed to the Information Commissioner for investigation.

4.6 The ICO also has joint working protocols with British Telecommunications, and with police forces around the country. The ICO's Investigations Unit liaises almost weekly with police forces, often at their request for advice. The unlawful disclosure of information from police systems is an issue of particular concern, as many professional standards units within the police are investigating corrupt practices by serving officers. Although such activities fall within the scope of section 55, the police prefer at present to arrest for malfeasance or corruption offences as these are punishable by imprisonment, an issue to which we return in paragraph 6.5.

Select Committee investigation into media intrusion

4.7 The ICO is not the only body to keep a watching eye on the encroachment of individual privacy. Early in 2003, the House of Commons Select Committee on Culture, Media and Sport conducted an investigation into privacy and media intrusion. Like the Information Commissioner in this report, the Committee was particularly concerned to focus on people who are 'not generally in public life'.

4.8 Among those giving evidence was Sun editor, Rebekah Wade, who claimed that self-regulation under the guidance of the Press Complaints Commission (PCC) had changed the culture in Fleet Street and 'in every single newsroom in the land'.[14] When asked whether she or her newspaper ever used private detectives, bugged people, paid the police or others for information they should not legally have, she said that subterfuge was only ever used in the public interest.

4.9 Pressed again by Committee member, Chris Bryant MP, on whether she ever paid the police for information, she replied, 'We have paid the police for information in the past.' Further probing about whether she would continue to pay the police in future was answered in her stead by her colleague, Andrew Coulson, who declared that 'We operate within the [PCC's] code and within the law and if there is a clear public interest then we will'.[15]

14 Select Committee on Culture, Media and Sport, 'Privacy and Media Intrusion', Minutes of oral evidence, Tuesday 11 March 2003, Ev 105.

15 Ibid., Ev 112.

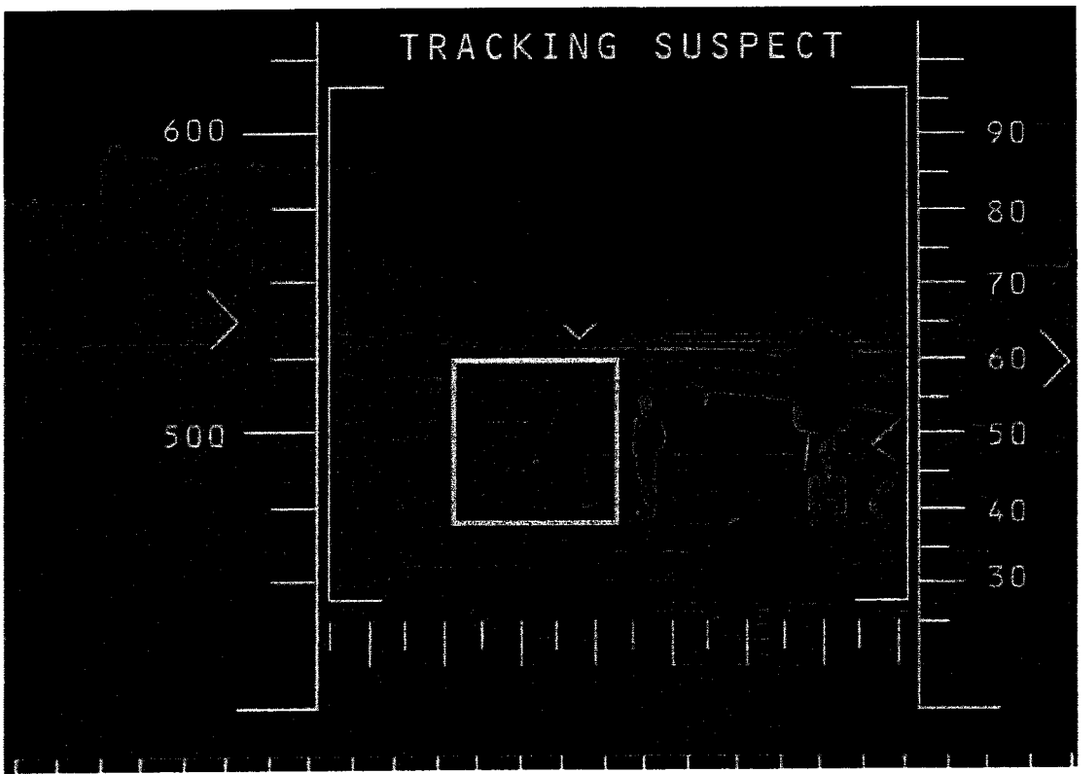
4.10 But in any case the Committee remained unconvinced by the media's apparent conversion to new codes of behaviour, and in its conclusions cited a number of reports detailing 'improper and intrusive gathering of data' that had appeared in the press itself.[16] They included:

A *Guardian* report in September 2002 indicating a data 'black market' and highlighting a private detective agency which had been found to have sold information from police sources to the News of the World, Daily Mirror and Sunday Mirror.

A *Sunday Telegraph* report in December 2002 that private detective agencies routinely tapped private telephone calls for the tabloid press, with some agencies deriving the bulk of their income from such work and such clients.

A report in *The Times* of January 2003 that the Inland Revenue's human resources directorate admitted there was evidence to show that some employees had sold confidential information from tax returns to outside agencies, without identifying the agencies concerned.

4.11 It is hardly surprising that the Select Committee concluded that these intrusive methods of data-gathering amounted to a 'depressing catalogue of deplorable practices'. We return to the Committee's recommendations in paragraph 7.19.



16 Culture, Media and Sport Select Committee, Fifth Report, Privacy and Media Intrusion, HC 458-1, 16 June 2003, para. 93

5 Breaking the law: the evidence

5.1 While the ICO had long suspected the existence of an organised trade in confidential personal information, charting the full extent of any unlawful activity is naturally fraught with difficulty. An insight into the scale of this unlawful market came in late November 2002 when the ICO was invited to attend a search of premises in Surrey executed under warrant by the Devon & Cornwall Constabulary. The raid concerned the suspected misuse of data from the Police National Computer (PNC) by serving and former police officers. Recognising the significance of documents listing vehicle registration numbers, the ICO investigating officer was able to link the apparently random numbers to vehicle checks carried out within the Driver and Vehicle Licensing Agency (DVLA) by two officials. Corruption was the stark conclusion and two investigations were subsequently launched: the ICO's Operation Motorman into data protection offences and later Operation Glade by the Metropolitan Police into possible corruption by police officers or civilian police employees.

Operation Motorman

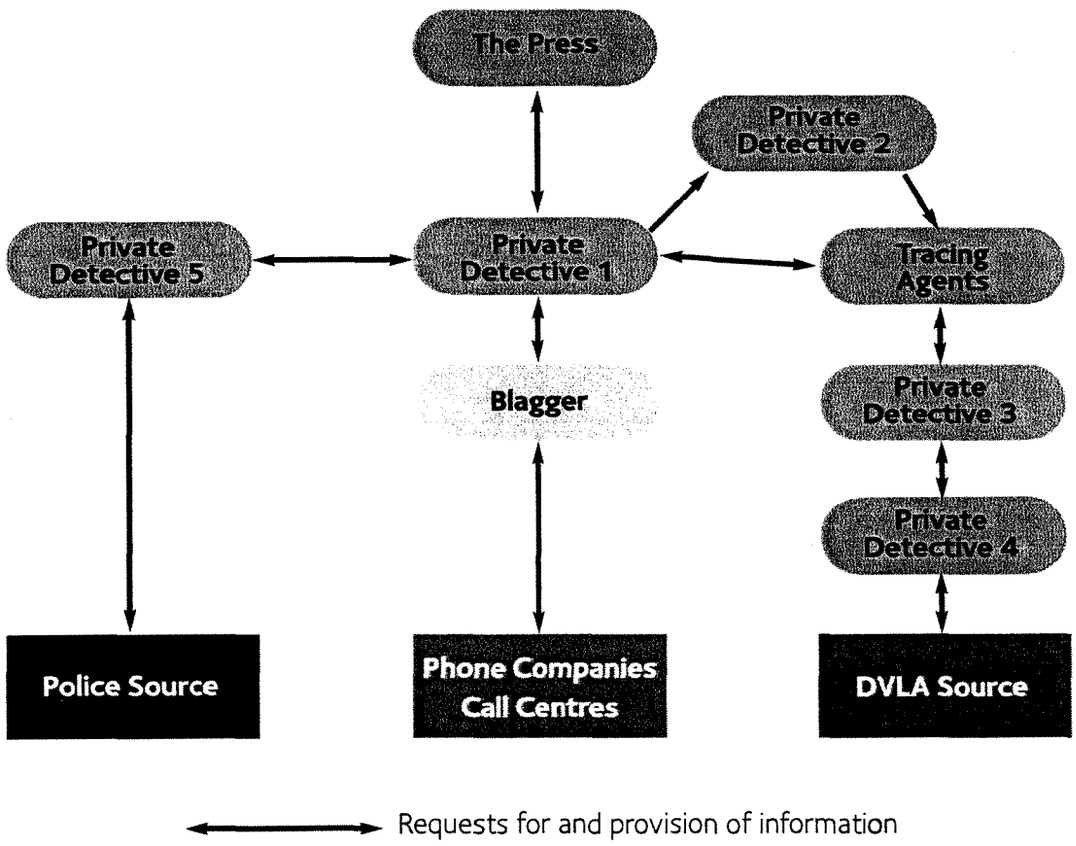
5.2 Further search warrants obtained by the ICO led the hunt to the premises of a private detective working from his home in Hampshire, and to two men who worked for him. Documentation seized from the detective's premises showed that he worked with a number of associates who were able to supply him with data unlawfully obtained from BT accounts as well as DVLA records. He also appeared able to obtain checks from the PNC (the specific offence that prompted Operation Glade). But it was the wealth of detail that was to prove so valuable to our knowledge of the illegal market in personal information: ledgers, workbooks and invoices detailing who had requested the information, precisely what information they were given, how much they were charged, and how much was paid to the associates who actually obtained the information.

5.3 This was not just an isolated business operating occasionally outside the law, but one dedicated to its systematic and highly lucrative flouting. Nor could its customers escape censure. Some of the information obtained (such as PNC checks, ex-directory telephone numbers and details of frequently dialled numbers) cannot normally be obtained by such businesses, by lawful means. Others – such as personal addresses – can be obtained lawfully only by the old footslogging means such as personal checks of the full electoral register.[17] The prices charged for some pieces of information raised questions about their provenance: either the price was too low for information obtained lawfully (as in the case of personal addresses), or it was high enough to indicate criminal activity (as in criminal records checks).

17 The edited register, by contrast, can be easily searched.

5.4 Documents seized during Operation Motorman and in other investigations have allowed the ICO to build up a clear picture of how the market in unlawful personal data operates. Case details provide evidence of who is buying the information and why, and who is obtaining and supplying the information. We also have some idea of how the suppliers operate, and the prices they charge.

Interaction of parties providing illegally obtained information to the press



5.5 On the demand side, the customers come from the following main groups:

- the media, especially newspapers
- insurance companies
- lenders and creditors, including local authorities chasing council tax arrears
- parties involved in matrimonial and family disputes
- criminals intent on fraud, or seeking to influence jurors, witnesses or legal personnel.

The media

5.6 Journalists have a voracious demand for personal information, especially at the popular end of the market. The more information they reveal about celebrities or anyone remotely in the public eye, the more newspapers they can sell. The primary documentation seized at the premises of the Hampshire private detective consisted largely of correspondence (reports, invoices, settlement of bills etc) between the detective and many of the better-known national newspapers - tabloid and broadsheet - and magazines. In almost every case, the individual journalist seeking the information was named, and invoices and payment slips identified leading media groups. Some of these even referred explicitly to 'confidential information'.

5.7 The information which the detective supplied to the newspapers included details of criminal records, registered keepers of vehicles, driving licence details, ex-directory telephone numbers, itemised telephone billing and mobile phone records, and details of 'Friends & Family' telephone numbers.

5.8 The secondary documentation seized at the same premises consisted of the detective's own hand-written personal notes and a record of work carried out, about whom and for whom. This mass of evidence documented literally thousands of section 55 offences, and added many more identifiable reporters supplied with information, bringing the total to some 305 named journalists.

5.9 Just as revealing were the interviews conducted with individuals whose privacy had been violated. As one would expect, they included a number of celebrities and others in the public eye such as professional footballers and managers, well-known broadcasters, a member of the royal household and others with royal connections, and a woman going through well-publicised divorce proceedings. But they also included people caught up in the celebrity circuit only incidentally, such as the sister of the partner to a well-known local politician and the mother of a man once linked romantically to a Big Brother contestant. Among this last group was a mother whose show-business daughter had featured in a number of lurid press stories about her private life and whose family was subject to intense media probing. Details of the mother's telephone calls and cars owned appeared among the private detective's ledgers and records of financial transactions.

5.10 A few of the individuals caught up in the detective's sights either had no obvious newsworthiness or had simply strayed by chance into the limelight, such as the self-employed painter and decorator who had once worked for a lottery winner and simply parked his van outside the winner's house. This group included a greengrocer, a hearing-aid technician, and a medical practitioner subsequently door-stepped by a Sunday newspaper in the mistaken belief that he had inherited a large sum of money from a former patient.

5.11 A number of those interviewed reported subsequent media intrusion into their lives, after their details had been passed on to the press. All were emphatic that they had not willingly supplied information about themselves, nor would they have consented to its release. Yet as we see later (in paragraph 6.7), despite the wealth of evidence collected in Operation Motorman, the outcome in the courts proved extremely frustrating.

Insurance companies

5.12 The insurance industry is another sector with an apparent incentive to acquire confidential personal data, particularly in respect of suspect claims. An insurance company with evidence of fraud might try to argue that its activities were necessary for preventing or detecting crime. But it would still have to prove that the activity was 'necessary' (implying that no other reasonable means were readily available) and that there was, in fact, a 'crime'. The mere possibility that an offence might have been committed would not provide a sufficiently robust defence, without corroborating evidence.

5.13 One case recently prosecuted by the ICO illustrates how even reputable businesses are breaching data protection legislation. The case involved a marine insurance claim for the loss of a boat sunk in deep water after a fire, which the insurance company had passed to a reputable City law firm for investigation. They in turn instructed a private detective (a former policeman) to investigate the claimant and gain information about his financial affairs, apparently to determine if he had a financial motive for sinking the boat himself. The detective then outsourced the work via an untraced contact to a man working out of a business centre in Cornwall.

5.14 Shortly afterwards, the claimant's 82-year-old mother received a telephone call purportedly from the Inland Revenue requesting her maiden name, which the caller said was needed to process a tax rebate for her son. She gave it without question. That same day, the caller made more bogus calls to the claimant's bank and eventually – after using the mother's maiden name as a security password and answering a further question about direct debits[18] - gained access to information about the claimant's bank accounts.

5.15 As soon as the claimant became aware of what was happening, he contacted the police who were able to trace the calls to the business centre in Cornwall. When it became clear that the case involved a breach in data protection legislation, the police passed it on to the ICO for further investigation. In subsequent court proceedings, the private detective pleaded guilty to obtaining data unlawfully. He received a one-year conditional discharge and was ordered to pay £1,200 in costs. Legal proceedings also took place against the man who actually 'blagged' the information. He pleaded guilty to eight offences. For two offences of obtaining personal information he received a fine of £250 per offence with no separate penalty imposed for the other six offences. He was also ordered to pay a contribution towards prosecution costs of £500.

18 The caller initially guessed wrongly that there was a direct debit order from the account, and the system shut him off. He called back immediately and this time made the correct guess, which gained him access to the bank account details.

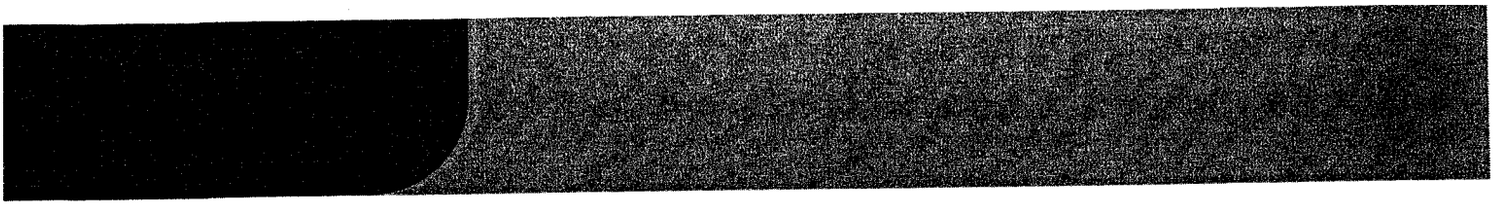
Lenders and creditors

5.16 Tracing debtors is another activity which relies on good, up-to-date personal information. To recover a debt from borrowers who have defaulted on their loans or financial commitments, creditors need a current address. While there are a number of legitimate means of tracing absconded debtors, these can often be time-consuming and expensive. For businesses, they include consulting the edited electoral register, employing tracing agencies that use data legitimately collected by credit reference agencies for the purpose of tracing debtors, applying for a court order to obtain information from judgment debtors, and consulting the Register of County Court Judgments. From April 2006 this register will be replaced by a register of judgments, orders and fines, which should make it easier for creditors to locate debtors and make decisions about pursuing the debt. The new register will include county court and high court judgments, fines and Child Support Agency liability orders. There are also proposals to include other similar court information on the register. In addition to these methods, local authorities may in some circumstances use internal information collected when undertaking their functions in other fields, and apply to neighbouring authorities when they are certain of a debtor's new location but not the actual address.

5.17 In a later section we look at how proposals for a new Data Disclosure Order may give creditors some help in tracing absconded debtors, while striking a balance between the legitimate rights of creditors and the individual's right to privacy. But it is clear from recent investigations by the Information Commissioner's Investigations Unit (ICIU) that a number of large, well-known lenders are outsourcing their debtor tracing to private investigating agencies who are less than scrupulous in the methods they use. The volume of work they undertake makes this a lucrative business. We know of one private investigation firm receiving some £50,000 a month from just one finance company for tracing new addresses at £35 a time, and £55 for a new employer and new address. The same firm was also undertaking checks for other companies, which gives some idea of the scale of operations.

5.18 Under current legislation, lenders and creditors have the responsibility to make sure that they do not knowingly or recklessly procure the disclosure of information by unlawful means. The same caveat applies to local authorities that seek to collect council tax arrears by outsourcing their tracing of debtors. As debt collection – including tax arrears – is not a criminal matter, the defence of preventing or detecting a 'crime' is not permissible.

5.19 Yet the ICO has evidence implicating local authorities in this unlawful trade. In a case that surfaced in March 2005, a job centre in Hull received a telephone call purportedly from a civil servant working in the section within the Department for Work and Pensions responsible for recovering overpayments. The man's apparent familiarity with office jargon and procedures allayed any suspicions that he might not be genuine. During the course of the conversation – which lasted over 90 minutes – he was able to gain personal information (mainly address and employment details) relating to 140 individuals living in no particular geographic area. A second call two days later was reported as bogus, and the matter referred to the ICO.



5.20 On investigation, the trail led to one of the individuals whose details had been obtained. She revealed that she had recently moved house without informing the council, and leaving her council tax bill unpaid. When contacted by the ICO, the council in question said that although most tracing was done 'in-house', the more difficult cases were referred to a tracing agent on a 'no trace-no fee' basis. The tracing agent involved charged £35 for a successful trace and £55 for an address and employment details. Search warrants executed at the agent's premises confirmed the prolific use of tracing agents by other local councils and by finance houses. When interviewed under caution, the tracing agent claimed to have outsourced the council work to another self-employed agent. As council records do not generally include their residents' national insurance numbers, he implied that absconding council debtors are harder to trace.

Family disputes

5.21 Privacy intrusions in matrimonial or family disputes represent another significant cause of complaints reaching the ICO, often with severe consequences for the individuals concerned. In one case prosecuted by the Information Commissioner, a private investigator had been engaged by a potentially abusive husband to track down his estranged wife, after the woman had determined to escape his campaign of harassment and start a new life with her daughter. Introducing himself as an official from the local health authority, the investigator had obtained details of the woman's whereabouts by telephoning her parents' medical centre and requesting their telephone number to check a prescription.

5.22 In another recent case, a father complained to the ICO about a possible breach of his privacy by the Royal Mail, although on this occasion there was insufficient evidence to prosecute. Again, the case involved a new start in life, offered by a couple to their daughter who had become entangled with a heroin addict. When the addict went to prison, the girl's father decided to take his daughter and his family as far away as he could. After selling his house at less than market value, he moved the whole family 200 miles, informing no one of their change of address except the Royal Mail's re-direction service. But when the addict came out of prison, he sent a text to his former girlfriend saying that he knew where she was and giving the new address.

5.23 Both these cases illustrate the damage that can result when personal information falls into the wrong hands. Yet all too often, data protection offences are characterised as trivial in nature and effect.

Fraud and criminal intent

5.24 In this age of widespread identify theft, much criminal attention is focused on acquiring personal details for the purposes of fraud. Such crimes are usually prosecuted by other authorities under legislation which carries greater penalties, such as the Theft Act. But some recent well-publicised cases have a clear data protection element that illustrates the growing seriousness of these offences.

5.25 Confidential personal information may also be of interest to criminals wishing to influence the outcome of trials, or those with a grudge to pursue. The ICO recently successfully prosecuted a private investigation firm for the offence of not registering under the Data Protection Act and for seven separate offences of obtaining personal information unlawfully. Among the individuals whose privacy had been violated was a woman who had been involved as a vital prosecution witness in a prolonged police enquiry. In an attempt to obtain her personal details, bogus calls were made to the utility company Powergen, and to British Telecommunications, seeking details of her 'Friends & Family' numbers. The investigator was later shown to have made 51 calls to 11 numbers on the list, but he failed in his attempt to gain access to her medical records: a bogus 'doctor' had telephoned her medical centre, claiming that her records were required by the Psychiatric Unit of a London hospital. Such repeated and prolonged intrusion naturally caused her great distress, and raised the spectre of possible witness intimidation or harassment.

The suppliers

5.26 The cases already raised give us some idea about the companies and individuals who actually obtain the data unlawfully. They are almost invariably part of the private investigation industry: private detectives (many are ex-police officers), tracing agents and their operatives, often working loosely in chains in which each link has its own speciality.

5.27 At the heart of prosecutions brought by the ICO as a result of Operation Motorman was a series of four conspiracies alleged against the Hampshire private detective and his associates. Two related to the unlawful obtaining of ex-directory telephone numbers, and two to unlawful searches of vehicle registration numbers at the DVLA. The private detective rarely obtained the information himself, choosing instead to outsource the work to his associates and adding a premium to the value of the information obtained as he sold it on. Occasionally, his associates would turn to him for information.

5.28 Among the detective's associates, one was – until his dismissal – an executive officer working for the DVLA at one of their local offices. This gave him access to the computer holding all information relating to motor vehicles throughout the United Kingdom, a truly valuable resource for the blagging community. Another associate was the director of a data research company involved in obtaining unlawful checks on DVLA data. A third operated from his flat on the south coast, impersonating employees of British Telecom to obtain information relating to individuals' telephone accounts. He would undertake 'conversions', putting an address to a telephone number and procuring ex-directory telephone numbers for people.

5.29 The insurance case involving the sunken boat revealed a similar pattern in which information was passed along a chain. In this particular case, the chain linking the ultimate client (an insurance company) to the man who actually obtained the claimant's bank account details went through a firm of City solicitors, a private investigator and one further untraced contact. When the ICO finally caught up with the man who had

made the bogus telephone calls (who had by then absconded from his business premises without paying the rent), he admitted to his part in the affair but refused to identify his 'contacts', apparently in fear of the consequences. He did, however, reveal that he had become involved some three years earlier, attracted by local advertisements promising earnings of between £500 and £1,000 a week. After meeting his contacts in a pub, he was set up in business by them and spent the next three years on the telephone, blagging information about people's private bank accounts. There may have been others like him, operating from the same business centre.

How they operate

5.30 As Operation Motorman and other conspiracies have demonstrated, confidential personal information is obtained in two main ways:

- through corruption, by paying employees who have access to the required information through their job; and
- by 'blagging' the information on the telephone, usually by impersonating the data subject or by impersonating another official from a different part of the organisation.

5.31 Material seized under warrant provides valuable insights into how the blaggers go about their task. Invariably premises searched yield training manuals, instructing new recruits in the tricks of the trade. The 'blagger' in the marine insurance case had even been sent on a course to learn how to get information out of systems and people.

> **'As with so many calls, it's all in the art of persuasion. You have to make that person want to tell you that address, even though we all know they shouldn't – it's as simple as that really ...'**
>
> 'A blagger's guide to obtaining information from a subject's bank or building society'

5.32 One of the more sophisticated manuals was recovered from the business premises of a private investigator in Middlesex. Diligently and with a certain wry cunning it takes the recruit through a trawl of next-door neighbours, family health services, employers, tax records, the employment service, social security, banks and building societies, local authority housing and tax departments, utility companies, and the Royal Mail. 'Know your jargon', is one of its recurring themes, and the importance of maintaining a strong-minded, confident approach.

5.33 Psychology is another weapon frequently brandished. Having characterised the staff of the old Department of Social Security as being 'subservient to the rules, rather lacking in personal character' and 'utterly paranoid about bogus callers', the manual offered the following advice:

> 'The way to con this type of person is to convince them that you are just as prim and proper as they are. Don't even bother calling them under the pretext that you are a cockney or an idiot, because you won't last five seconds. They deal with idiots and layabouts all day, so ring them in the style of a keen little civil servant who wants to learn to solve their problems instead of relying on senior staff at another other office. Speak with a clear, confident manner. Be polite and friendly at all times as rudeness will not work here.'

5.34 The manual concluded with more than 15 pages of sample scripts to use when trying to obtain information from a telephone call, for instance, and for discovering the relationship between two people by impersonating a public transport lost property office. All the scripts are frighteningly plausible, as can be seen from the extract contained in Annex B. Recorded telephone conversations to call centres confirm how easy it can be to circumvent security questions designed to check the caller's identity. Some blaggers make repeated calls to the same call centre adopting different identities (and occasionally different genders) as they seek to 'check' personal details such as their current employers. Usually the calls will be taken by different personnel but in rare cases the caller's voice will be recognised and further information refused.

What they charge

5.35 Operation Motorman also uncovered details of what the ultimate customers are charged for personal information and occasionally, how much of this was profit, and how much went to the agent actually sourcing the information. Prices charged to the customer ranged from £17.50 for finding an address for someone listed on the electoral register, up to £500 for conducting a criminal records check and £750 for obtaining mobile telephone account details. These charges are shown in Table 1 below.

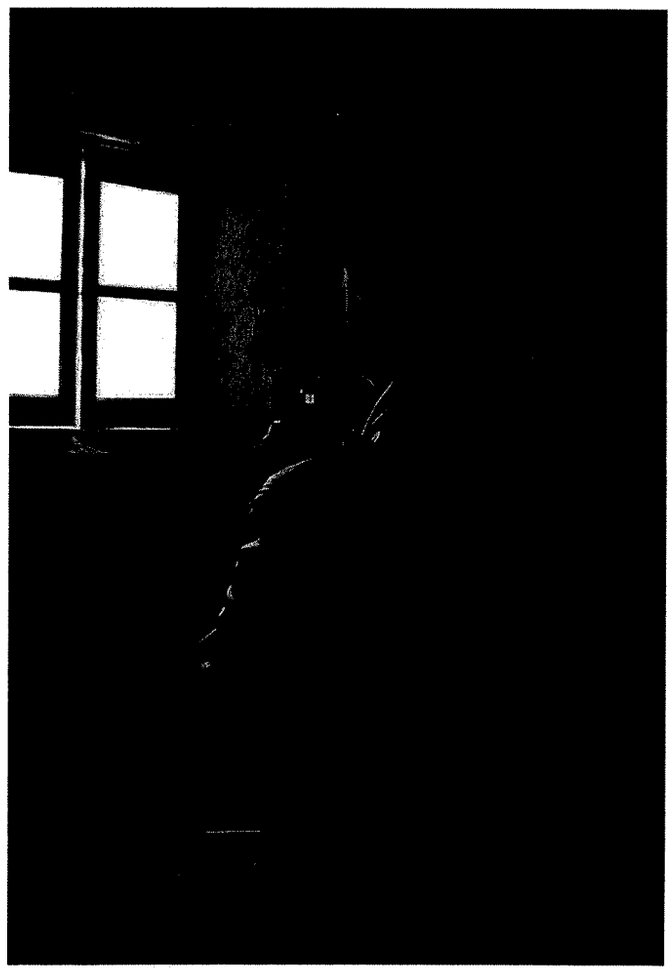
TABLE 1: Tariff of charges in Motorman Case

Occupant search/Electoral roll check (obtaining or checking an address)	not known	£17.50
Telephone reverse trace*	£40	£75
Telephone conversion (mobile)*	not known	£75
Friends and Family	£60 – £80	not known
Vehicle check at DVLA	£70	£150 – £200
Criminal records check	not known	£500
Area search (locating a named person across a wide area)	not known	£60
Company/Director search	not known	£40
Ex-directory search	£40	£65 – £75
Mobile telephone account enquiries	not known	£750
Licence check	not known	£250

Scale

5.36 The scale of activity undertaken can also be gauged from the invoices that passed between buyers and suppliers in the Motorman investigations. In just one week in 2001, for instance, a named journalist on the news desk of a Sunday newspaper was billed for 13 occupant searches, two vehicle checks, one area search and two company searches, making a total bill of £707.50 plus £123.81 VAT. The following January, the Hampshire detective paid one of his company associates £1,540.00 for 22 vehicle checks at £70 a time. These would have netted him a profit of £1,760. This transaction does not show how much was actually paid to the contact within DVLA.

5.37 Documents seized from the tracing agent working for finance houses and local councils revealed that one agent was invoicing for up to £120,000 per month of positive tracing.



6 Assessing the damage

6.1 We now turn to the damage inflicted by this unlawful trade in personal data. From the cases discussed, much of the harm to individuals is self-evident in terms of the aggravation, grief and personal mischief suffered. Having the press camped on your doorstep or receiving intrusive calls to self, family or friends is an experience few enjoy, especially if they have done nothing to court media attention. Having your address released to those who may wish you harm may be even more disturbing. Respecting the privacy of the individual is, and must, remain a cornerstone of data protection legislation.

6.2 For legal and commercial reasons, organisations have an equally strong interest in keeping their personal information secure. Indeed, the law recognises the 'data controllers' as the victims of this crime – the government departments, agencies, banks, telephone companies and others whose store of personal data is systematically breached. The seventh data protection principle set out in the 1998 Act makes it a legal requirement that 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data'. This requirement is underpinned by international standards in information security, such as ISO/IEC 17799:2005 and ISO/IEC 27001:2005. From discussions and correspondence with such bodies as the Department of Health, the Department for Work and Pensions, Department for Education and Skills, and the Government's Council of Chief Information Officers, the Commissioner is very encouraged that his concerns about the risks to security are clearly shared. As well as ensuring high levels of security, strong support has been expressed for a much tougher approach to deter and punish those involved with illegal disclosure.

6.3 In a world where face-to-face transactions are no longer the norm, it is increasingly important that people should have confidence in the security of the organisations holding their personal information. Businesses cannot and must not take good security for granted. It is similarly vital for fostering the take-up of e-government services.

6.4 The key commercial role played by an organisation's reputation for security was vividly demonstrated in 2005 in the United States, where a number of high-profile security breaches undermined consumer confidence. In one case, millions of dollars were wiped off the stock-market value of the company concerned, consumer data broker ChoicePoint Inc. Acknowledging that the personal financial records of more than 163,000 consumers in its database had been compromised, the company agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle the Federal Trade Commission's charges that its security and record-handling procedures violated consumers' privacy rights and federal law. The FTC chairman spelt out bluntly that 'Consumers' private data must be protected from theft'.[19]

19 Federal Trade Commission press release, 26 January 2006.

6.5 There is another principle at stake as well: respect for the law. The fact that prison is not currently an option for persons convicted of section 55 offences belittles the offence and masks its true seriousness, even to the judiciary. Whenever possible, the police will arrest for malfeasance or corruption offences rather than section 55 offences, as the latter are non-arrestable offences and carry a fine only. The police tell us that they would prefer to use section 55 as the basis for their investigations – and believe that they would achieve quicker convictions – if the offence carried the possibility of a prison sentence. The threat of imprisonment would also, in their view, act as a suitable deterrent.

6.6 In the absence of custodial sentences, the penalties imposed on those found guilty of data protection offences have often been slight. As we have seen, in the case involving an insurance claim for a sunken boat, the private detective who pleaded guilty to obtaining data unlawfully and disclosing information relating to the claimant's bank account received a one-year conditional discharge, and an order to pay costs of £1,200.

6.7 The outcome of prosecutions brought as a result of Operation Motorman proved even more frustrating. Parallel investigations launched by the police (acting on information provided by the ICO) had uncovered evidence of the unauthorised supply of information from the Police National Computer by a civilian police employee. The Crown Prosecution Service (CPS) charged four people with corruption offences. Ultimately two pleaded guilty to corruption charges and two to specimen data protection charges under section 55 of the Data Protection Act 1998. As the corruption charges carry a possible custodial sentence, these were given precedence over the Motorman cases. The CPS prosecutions resulted in some convictions, including those of the 'lesser' offences under section 55, but the court was not able to impose any sentence stronger than a conditional discharge, because of sentencing in a connected but separate case.

6.8 This was a great disappointment to the ICO, especially at it seemed to underplay the seriousness of section 55 offences. It also meant that it was not in the public interest to proceed with the ICO's own prosecutions, nor could the Information Commissioner contemplate bringing prosecutions against the journalists or others to whom confidential information had been supplied.

7 Conclusions and recommendations

7.1 Evidence collected by the ICO points to a flourishing and unlawful trade in confidential personal information by unscrupulous tracing agents and corrupt employees with access to personal information. Not only is the unlawful trade extremely lucrative, but those apprehended and convicted by the courts often face derisory penalties. The situation is already serious and underlines the need for stronger sanctions against those who breach the Data Protection Act 1998. The Government's plans for increasingly joined up and e-enabled public sector working make the change even more urgent.

7.2 These offences occur because there is a market for this kind of information. At a time when senior members of the press were publicly congratulating themselves for having raised journalistic standards across the industry, many newspapers were continuing to subscribe to an undercover economy devoted to obtaining a wealth of personal information forbidden to them by law. One remarkable fact is how well documented this underworld turned out to be.

7.3 The press are not the only drivers of this market, of course. This report highlights many other businesses which regularly turn to private investigation firms and through them to the shadier end of the tracing market, requesting confidential personal information they must know or suspect has been unlawfully obtained. It may only be exceptions on the fringes, but it is clear that insurance companies, solicitors, local authorities, finance companies and other lenders are implicated in this trade. And sections of the private investigation industry appear willing to flout the law and provide the information requested.

7.4 The evidence also demonstrates that we are all equally at risk of having our privacy invaded. In cases sparked by media interest, for instance, the targets include celebrities and their families but also people with only the slimmest connection to the stars, and some individuals who have simply no idea why their personal details might be of interest to anyone. And while the invasion of privacy can cause distress to many, for some people it can have more sinister implications when private details fall into the wrong hands. The cases we have investigated include an abusive husband able to track down his ex-partner's whereabouts through her parents' medical records, and a prosecution witness to a lengthy trial who feared subsequent harassment.

7.5 As currently expressed, the law relating to these offences is perfectly clear. Furthermore, it is framed in a way that applies to those who request the disclosure of personal data and those who supply it, including any intermediaries in the chain. The problem lies in the inadequacy of the penalties which the courts are able to impose.

A custodial sentence

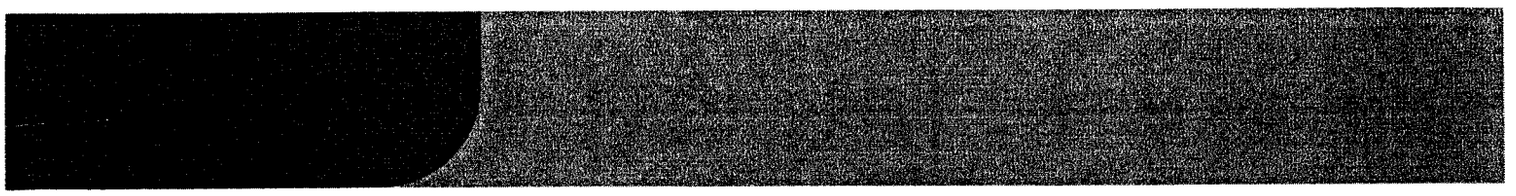
7.6 The Information Commissioner's ultimate aim is not to add to the number of prosecutions but rather to discourage this unlawful trade in the first place. This can be achieved only by increasing the penalty in a way that underlines the seriousness of the offence and makes reputable businesses and individuals reflect on the possible consequences of their actions: by introducing the possibility of a custodial sentence for convictions obtained in the Crown Court and the Magistrates' Courts.

7.7 For convictions obtained on indictment, the penalty set out in the Identity Cards Act provides a helpful precedent. For unlawfully disclosing confidential information, the Act states that 'A person guilty of an offence under this section shall be liable, on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both'. Two years would, of course, represent the maximum term, and would not be appropriate in the majority of cases. For summary convictions, a lesser maximum custodial sentence of six months would be appropriate. These changes could be achieved by amending section 60(2) of the Data Protection Act 1998, which sets out the penalties for offences under the Act. Further amendment would be necessary to limit the custodial sentence to convictions for section 55 offences, and not to other data protection offences, such as non-registration.

7.8 **The Information Commissioner recommends an amendment to section 60 (2) of the Data Protection Act 1998, increasing the penalty for section 55 offences committed under the Act to a term of imprisonment not exceeding two years, or to a fine, or to both, for convictions on indictment; and to a term of imprisonment not exceeding six months, or to a fine, or to both, for summary convictions. The Information Commissioner calls on the Lord Chancellor, as the Minister responsible for data protection policy, to introduce the necessary legislation into Parliament as quickly as possible.**

Stifling demand

7.9 With stronger penalties in place, it is also necessary to send out a clear message that all those involved in the chain of supply may be committing an offence under section 55. In the past, some private investigators have tried to distance themselves from criminality by using self-employed tracing agents or by sub-contracting the work to other enquiry agents. But prosecutions have subsequently proved that outsourcing the work in this way does not preclude the principal from being tried and convicted for the offence. In one case involving a chain of several intermediaries between the ultimate client and the tracing agent, the Information Commissioner is in the process of cautioning a partner in the law firm acting for the client. While in other circumstances an actual prosecution might have been considered appropriate, the partner concerned will also face the possibility of disciplinary action by the Law Society.



7.10 Any business or individual involved with obtaining, supplying or buying personal information about private individuals needs to be aware of the risks of committing a section 55 offence. This includes principals, agents, associates, solicitors, tracing agents and every other link in the chain. They should restrict themselves to information which they are confident has been lawfully obtained. Otherwise, it is only a matter of time before they find themselves charged with this offence. It is in line with the Information Commissioner's new regulatory strategy to prosecute such 'commercial' offenders more actively.

Main players

7.11 The next series of recommendations are aimed at some of the main players whose actions can do much to stem the traffic in confidential personal information: the Security Industry Association, the Association of British Investigators and the Press Complaints Commission.

Security Industry Authority

7.12 The Private Security Industry Act 2001 empowers the Security Industry Authority (SIA), as a statutory body, to introduce compulsory licensing for private investigation firms. The SIA is continuing to consult a range of interested parties on its proposed licensing regime, and is currently conducting a regulatory impact assessment into its proposals. Licensing is part of a wider remit seeking to raise the professional standards and skills of the security industry generally, and to promote good practice.

7.13 The Information Commissioner recommends that the SIA should include a caution or conviction for a section 55 offence among its grounds for refusing or revoking the licence of a private investigation agency. The SIA should make it clear that private investigators who have been cautioned or convicted for these offences should be automatically deemed unfit to hold a licence and therefore effectively prevented from continuing in business. The licensing requirements should apply retrospectively, affecting any private investigator with convictions or cautions for data protection and other offences during the five years prior to the new system coming into force. The ICO proposes to work closely with the SIA to make sure these offences are given their proper weight.

Association of British Investigators

7.14 The Association of British Investigators describes itself as the 'leading professional body, working with investigators to promote members and the profession'. It provides a range of training and other support services to its members. As a clear demonstration of how seriously it is taking the imminence of SIA licensing, the ABI is currently developing a National Occupational Standard for Investigation, which stresses - at least in general terms - the importance of complying with all relevant laws and legal requirements. The Information Commissioner welcomes its reported support for statutory regulation.[20]

20 See The Economist, 10 Feb 2006.

7.15 The Information Commissioner recommends that the Association of British Investigators should:

- **Condemn unequivocally any activity which breaches section 55.**
- **Expel any member cautioned or convicted under section 55.**
- **Publicise this report to its membership.**
- **Organise training to make sure that its members do not inadvertently break the law.**
- **Extend the National Occupational Standard for Investigation to include explicit reference to section 55.**
- **Support the proposal outlined above that the SIA should refuse or revoke a private investigator's licence for anyone convicted or cautioned for a section 55 offence.**

7.16 The Commissioner proposes to discuss with the ABI over the next six months how these recommendations might best be put into practice.

Press Complaints Commission

7.17 Increasing the penalties for section 55 offences should not in any way fetter the press in the lawful pursuit of its stories. Nor does the Information Commissioner propose any change to the existing public interest defence (under section 55 (2) (d)), which exempts those able to demonstrate that obtaining, disclosing or procuring a particular piece of confidential personal information is in the public interest.

7.18 In the conclusion to its inquiry into privacy and media intrusion, the Select Committee called for an investigation by the Press Complaints Commission (PCC), ideally in cooperation with the Information Commissioner and the Police Complaints Authority.[21] The Committee further called on the Information Commissioner 'to make sure that all public and commercial entities are aware of their responsibilities under the Data Protection Act and put in place adequate training, guidance and other mechanisms to ensure that those responsibilities are fulfilled.'[22]

7.19 Following publication of the Select Committee's report, the Information Commissioner brought to the attention of the PCC's Chairman an outline of the evidence that was emerging during the Motorman investigation. As was made clear, certain journalists associated with certain newspapers and magazines were behaving in an unacceptable way, especially in the light of the Select Committee's recent condemnation. After a further meeting and correspondence, the PCC issued a Note reminding the press of its data protection obligations, including the possibility of committing an offence when obtaining personal information.

---

21 Culture, Media and Sport Select Committee, Fifth Report, Privacy and Media Intrusion, HC 458-1, 16 June 2003, para. 95.

22 Ibid, para. 97.

7.20 **The Information Commissioner recommends that the Press Complaints Commission (and its associated Code of Practice Committee of Editors) should take a much stronger line to tackle any involvement by the press in the illegal trade in personal information.** Following publication of this report the Commissioner proposes to raise the issue again with the PCC and will be asking for firm proposals within six months.

7.21 A fair balance must be struck between allowing journalists the freedom to do their job properly and protecting individual privacy. But there are lines which must not be crossed. Section 55 already includes clear defences, where for example it was necessary to prevent or detect crime or where obtaining a particular piece of confidential personal information in the course of genuine investigatory journalism can be justified as being in the public interest. **The Information Commissioner will not hesitate to take action against any journalist identified during the Motorman investigations who is suspected in future of committing an offence.**

Tracing debtors

7.22 While this report in no way condones the behaviour of debtors who abscond without informing their creditors, tracing agents must stay within the law like everybody else. The fees charged by many tracing agents for tracing such debtors suggest that they may be obtaining current addresses and employment details by unlawful means. 'No-trace no-fee' arrangements are especially open to abuse.

7.23 In 2003, the Department for Constitutional Affairs proposed a new court order allowing creditors to require information from a third party. Known as the Data Disclosure Order (DDO), this would enable the creditor to apply to the court to seek information on a judgment debtor who had failed either to respond to the judgment or to comply with court-based methods of enforcement. Under the new order, information would be sought from relevant third parties in both public and private sectors, among them HM Revenue and Customs, the Department for Work and Pensions, banks and credit reference agencies, to help make an informed choice about how to enforce a judgment.

7.24 **The Information Commissioner supports any such efforts to develop legitimate means for tracing debtors and enforcing debts, providing an appropriate balance is struck between respecting the legitimate interests of creditors and the privacy rights of individuals.**

7.25 **The Information Commissioner further recommends that the Office of Fair Trading should amend its 2003 Debt Collection Guidance – which is directly linked to fitness to hold a consumer credit licence - to include an explicit condemnation of activities that breach section 55.** The guidance exerts a direct influence over whether creditors, debt collectors and others in the finance industry are deemed fit to hold a consumer credit licence.

Raising awareness and standards

7.26 The primary thrust of this report so far has been to argue the case for a substantial increase in the prescribed penalty for section 55 offences. The threat of imprisonment will undoubtedly carry home the seriousness of the offences, deter those who may be tempted to engage in illegal activity and emphasise to reputable businesses the importance of staying within the law.

7.27 We also seek to raise awareness of the nature and extent of the illegal trade in personal information. Individuals must recognise how important it is to safeguard their own information as far as possible and disclose no more than is absolutely necessary. Businesses and other organisations which process personal information are equally at risk, reinforcing the ICO's emphasis on the high value of effective security measures.

7.28 The Information Commissioner will continue discussions with all parties affected by these issues, with a view to encouraging good practice and making sure that all parties are aware of their obligations under the law. To protect themselves and their customers against 'blagging', businesses need to train call centre staff so that they are aware of the risks. They also need to look at their procedures for handling suspect communications, calling back to a known telephone number in doubtful cases and reporting calls they suspect to be bogus. As always, they will need to strike the right balance between improving security and maintaining customer satisfaction. Improvements in security go hand-in-hand with increased penalties for those who seek to obtain personal information by unlawful means.

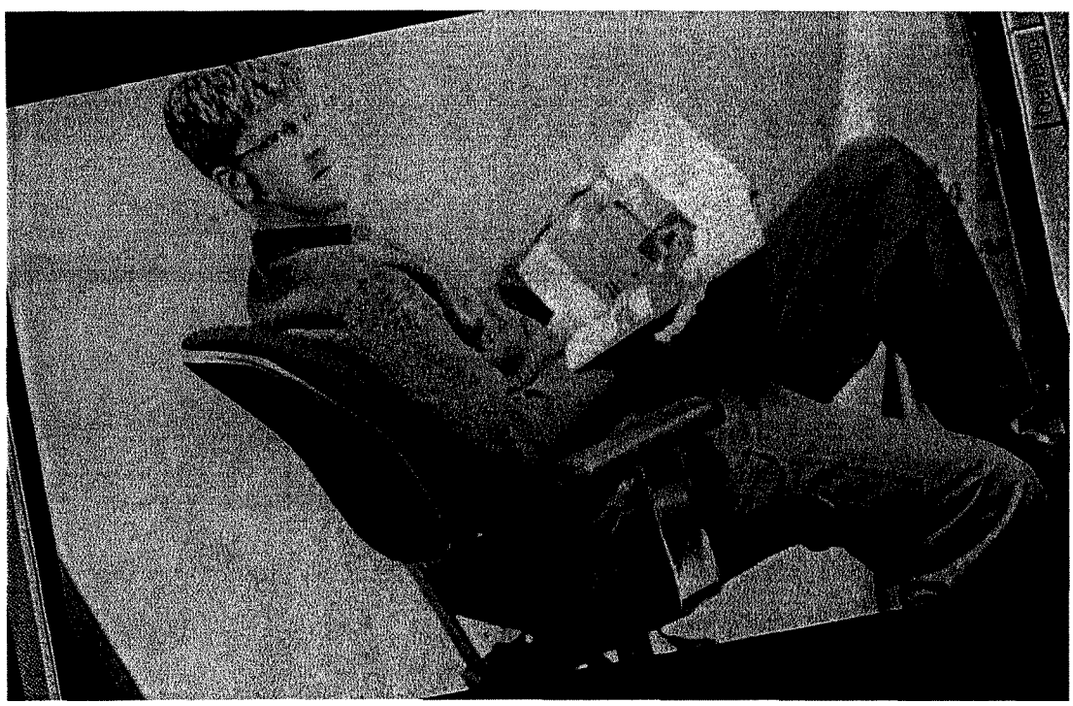
Other regulatory and professional and bodies

7.29 More generally, the Information Commissioner recommends that all relevant regulatory and professional bodies should take a strong line to tackle any involvement in the illegal trade in personal information.

7.30 The Information Commissioner has identified a number of regulatory and professional organisations which appear to be in a position to exercise control or influence over those who may engage in the buying or selling of personal information. This list is not exhaustive. Many of the information-gathering activities undertaken by those working within these spheres may be entirely legitimate. But as this report has clearly demonstrated, some may involve illegality, albeit sometimes at the fringes of the trade or profession, and sometimes at a remote distance, on the part of sub-contractors, agents or associates. It is vital, therefore, that all the bodies able to influence or control behaviour should raise awareness of the existing law, and take steps to deter illegal conduct at any point in the chain.

7.31 With the publication of this report, the Commissioner is therefore writing to the bodies listed below with the following specific questions in relation to their members or those they regulate:

- **What steps will you take to publicise this report among your members or those you regulate?**
- **Are you willing to condemn unequivocally the commission of offences under section 55 of the Data Protection Act, and if so, how will you do this?**
- **In six months' time, will you let the Information Commissioner have details of any changes made or in prospect to the relevant disciplinary rules, codes of practice or other instruments (statutory and self-regulatory), with the aim of improving your control or influence over the illegal buying and selling of personal information?**



Media bodies

- BBC (Producers Code)
- National Union of Journalists
- Newspaper Publishers' Association
- Scottish Newspapers Publisher's Association
- Newspaper Society
- Ofcom
- Periodical Publishers Association
- Society of Editors

Finance Industry

- Association of British Insurers
- British Bankers' Association
- Consumer Credit Association
- Consumer Credit Trade Association
- Credit Services Association
- Finance and Leasing Association
- Financial Services Authority

Professional bodies

- Local Government Association
- Convention of Scottish Local Authorities
- Welsh Local Government Association
- Northern Ireland Local Government Association
- Incorporated Law Society of Northern Ireland
- Law Society
- Law Society of Scotland
- Police Federation of England and Wales
- Scottish Police Federation
- Association of Chief Police Officers
- Association of Chief Police Officers in Scotland
- Police Federation for Northern Ireland
- Police Superintendents' Association of England and Wales
- Police Superintendents' Association of Northern Ireland
- The Association of Scottish Police Superintendents

The wider picture

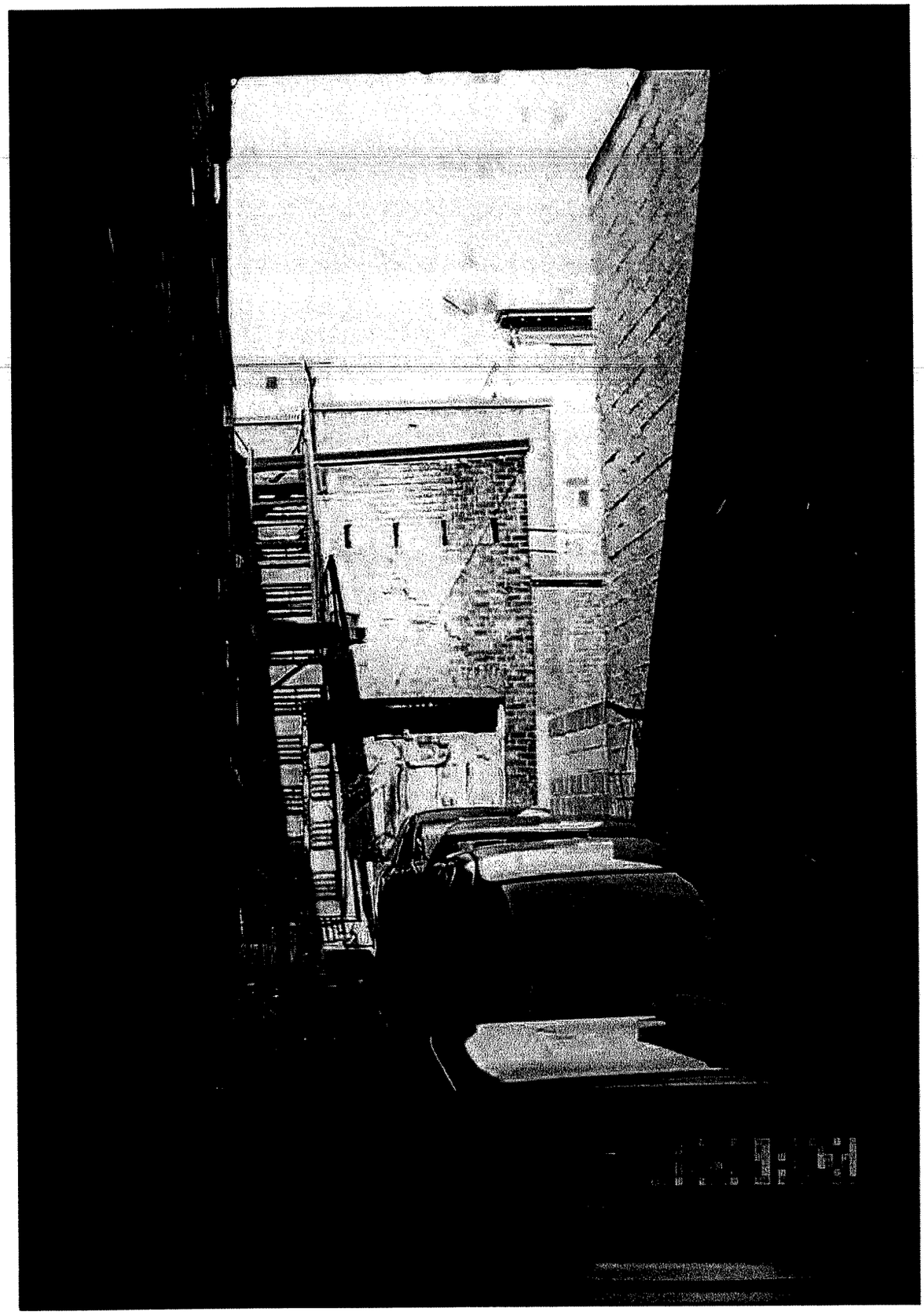
7.32 The Information Commissioner also intends to send this report to consumer and citizen organisations and to the consumer media, drawing their attention to the problems and inviting general or specific evidence about the nature and extent of the unlawful trade in personal information. The bodies to be consulted in this way include Citizens Advice and Citizens Advice Scotland, the National Consumer Council and its regional equivalents, Which? and the 'You and Yours', 'Watchdog' and 'Money' programmes.

Next steps

7.33 Data protection is ultimately about promoting enlightened self-interest - of the organisations that process personal information, and of the individuals whose personal details they process. As this report has shown, we all have a responsibility to keep those systems secure and to remain vigilant in case of breaches in security. Data protection laws set out to protect the rights of individuals and beyond that, to build confidence in the organisations to which we entrust our personal details. Government, business and the courts need to recognise the importance – and the benefits – of taking information rights seriously.

7.34 Many organisations are in a position to control or influence those who may be tempted – directly or indirectly - to participate in, or support, this illegal trade. The Information Commissioner will send this report to each of the bodies named in the recommendations, and follow up and publicise their responses. The report will also be publicised more widely. **The Information Commissioner anticipates publishing a follow-up report 6 months after publication of this report, to document responses and progress.** He also suggests that a Parliamentary Select Committee – either Culture, Media & Sport or Constitutional Affairs - might then wish to examine the issues raised in this report and the responses to it.

[redacted]



Annex A:

Table of prosecutions brought by the Information Commissioner

Date of Hearing	Court	Defendant	Result	Offence	Sentence	Costs
18/11/02	Brecon Magistrates Court	Karen Pritchard	Convicted	2 x 5 (6), S55 x 34, TICs x 348	£150 x 2, £50 x 34	£600
18/11/02	Brecon Magistrates Court	Karen Pritchard	Convicted	S55 x 34	£50 x 34	£0
18/11/02	Kingston Crown Court	Raphel Codrington	Convicted	5 (6) x 2, S55 x 8	£50 x 10 = £500	£1500
23/04/03	North Sefton	Neil Cartwright	Convicted	55 (1) Obtaining	£150	£100
28/04/03	Hastings Magistrates Court	Mark Brasier	Convicted	S55 (1) Obtaining	£300 fine	£650
23/07/03	Bow Street Magistrates	Leo Ketchin	Convicted	S55 x 3 Obtaining	£500 x 3	£800
22/09/03	Nottingham Magistrates Court	Sylvia E Soltysik	Withdrawn	13 x Obt, 13 x Discl (DPA 98)		
06/10/03	Warwick Crown Court	Stephen Mayall	Convicted	1 x Obt & 10 TICs Obt (DPA 98)	2 year conditional discharge	
20/10/03	Birmingham Magistrates Court	Abdullah Dervish	Convicted	8 x Obt, 2 x Discl, 165 TICs (DPA 98)	£1000 per offence = £10,000	£5,000
07/11/03	Tameside Magistrates Court	Darren Paul Graham	Convicted	55 (1) Obt x 2	£150	£150
10/11/03	Nottingham Crown Court	Zbigniew A Soltysik	Convicted	13 x Obt, 13 x Discl, 548 TICs (DPA 98)	£100 x 26 offences	£1000
07/01/04	Wallasey Magistrates	Bernic Security / Bruffell	Convicted	1 x Obtain	£1000	£1000

Date of Hearing	Court	Defendant	Result	Offence	Sentence	Costs
01/04/04	Peterborough Magistrates Court	Colin Rex	Convicted	1 x Obtaining	12 month Conditional Discharge	£300
19/04/04	Leeds Magistrates	Mark Hoy & MKN Legal & Financial Svcs Ltd	Convicted	12 Obtain 4 attempts to obtain x 2, 32 total	Co. £100 p/off Mr Hoy £50 p/off £2900 in total	£500
26/04/04	Cardiff Magistrates Court	Paul McColl	Convicted	55 (1) Obt x 5	£500 each offence	£3000
11/05/04	Portsmouth	Peter Mark Bascombe/Brays Detective Agency	Other	Obtaining and disclosing x 2 of data (x 2)		£0
08/09/04	Richmond Upon Thames	Derrick Ellis	Convicted	55 (1) x 6 – 3 Obt, 3 disclose	£200	£200
07/10/04	Richmond Upon Thames	Managed Credit	Convicted	55 (1) x 2 Obtain	£100 fine per offence	£200
08/10/04	Skegness Magistrates Court	Christopher Cooper	Convicted	55 (1)	Conditional discharge	£600
10/01/05	Shrewsbury Magistrates Courts	David Bufton	Convicted	2 x Obt (S55)	18mth conditional discharge	£200
08/02/05	Leeds Crown Court	Stanley Ronald Julien	Withdrawn	55 (1)		
23/02/05	Liverpool Crown Court	Mrs Susan F Stansfield	Convicted	S55 (1) 3 x Obt	£500 for each offence	£500
03/06/05	PF Dundee	Gillian McFarlane		S55	£500	
15/09/05	Liverpool Magistrates Court	Mr David J Hounslea	Convicted	S55 (1) 2 x Obt, 1 x Discl.	Absolute discharge	£0
19/10/05	Brent Magistrates	Pearson	Convicted	17 (1) & 55 (1) x 7	£500 plus £750 x 7 (£5750)	£600
12/01/06	Croydon	David Sibley	Convicted	S55	12 mths conditional discharge	£1200

Annex B:

Extract from blagger training manual

FOR DISCOVERING THE RELATIONSHIP BETWEEN 2 PEOPLE

British Rail/London Transport Lost Property Blag

This is to discover what connection the person you are ringing up has with the person under investigation OR what the address of the person under investigation is from friends and/or relatives.

You can therefore use this blag to discover the nature of a relationship.

You go on as British Rail (or London Transport) Lost Property.

In this example the telephone number you wish to establish connection with is 081-450 4321 and belongs to Mr Wilson.

4321 **Hello.**

Agent/BR **Hello. Is Mr Wilson there please?**

[Or if you only have the telephone number you go straight onto the bit where you explain who you are and why you want the information. "Hello, it's British Rail lost property here."]

Respondent **...Yes, speaking. Who's calling?**

Agent/BR **British Rail Lost Property.**

I'm sorry to bother you but we've had a [Wallet, Purse, Filofax etc] **handed into our office belonging to a Mr** [Give subject's name] **but no address. We wish to return the item as quickly as possible.**

We did, however, find your [name and telephone] **number in the diary in Mr** [Subject] **wallet/handbag so we assumed you knew Mr** [Subject] **and could therefore give us any useful information that could help get this back to Mr** [Subject]. [DO NOT ask directly for the address or phone number as this is too direct.]

[At this stage they may offer you a phone number or address or tell you where they can contact the subject. Remember as you're supposedly handling someone's personal affects for security, you should ask what their relationship is to your subject. Be polite. Also as nobody is familiar with BR lost property they would have no idea how the department works. Therefore a call back can be easily avoided. Tell them "that you presently have 3 calls on hold, and you need to sort it out now."]

Remember if you need other info make light conversation on the subject that you're interested in. Don't forget that all you're supposedly trying to do is to return lost property.

Extract from blagger training manual

OBTAINING SOMEONE'S BANK DETAILS DIRECTLY

TO: THE SUBJECT

AS: BT ACCOUNTS

Subject **Hello.**

Agent **Good afternoon. British Telecom Accounts Section. May I speak to Mr** [Subject]?

Subject **Speaking.**

Agent **Regarding the last bill relating to telephone number 081-123 4567, there is a possibility that your meter may have been faulty and overrunning. We've had complaints from quite a few people on the same side of the road as yours about abnormally high bills. Have you noticed that your last quarter bill was abnormally higher than usual for a quarter?**

Subject **Yes, it was a bit high.**

Agent **Our engineers have notified us, from various meter tests, that you were probably overcharged 537 units over and above that which you used. This comes to a credit refund of 4.02p/unit x 537 units** [tap it out on a calculator next to the phone for the subject to hear], **this equals a total refund of £21.59.**

We can credit your account on the next telephone bill next quarter or pay the money directly into your account today by Direct transfer.

Which would you prefer?

[Most people go for the bank option as this ensures that they get the money quicker. If the subject opts for the credit to the next BT bill, correct yourself and say "Oh, I'm terribly sorry but I've just realised that for amounts less than £30 our department policy is to credit your bank account or building society directly".]

Can I take your details please and I'll get the transfer made this afternoon?

[Wait for the subject to respond before asking the next question as the subject may give you all the info without needing to be asked.]

Your bank is ....? and the branch address? And the account number is?

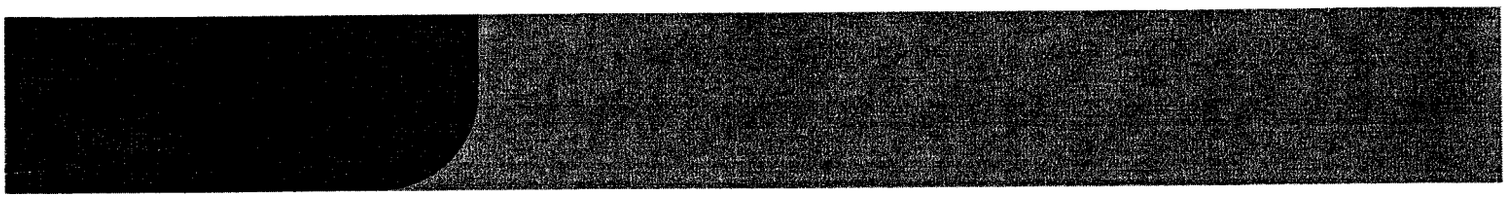
Do you have any other banks or building societies we could use to transfer the money to as [the first given bank] **tends to take a bit longer to pay into than some of the others?**

[Then take details of any other banks and building societies in the same fashion]

You should get the credit through tomorrow or the day after. Thanks. Bye.

If you're asked for your telephone number say "Freephone BT Account North London" [Replace London with the relevant town].

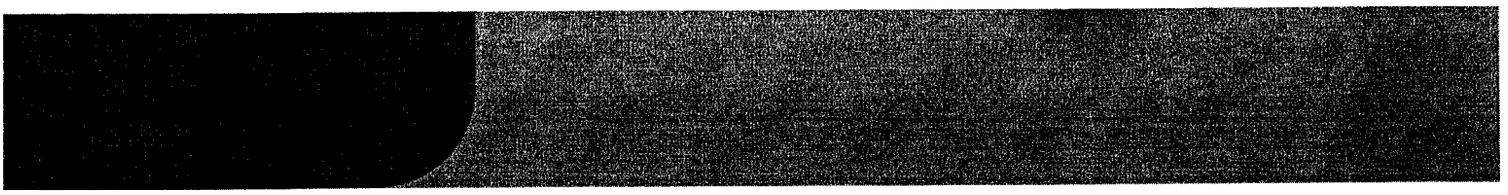
If you're asked for your name just say "Mrs Adams, but anyone will be able to help you when you call our section as we are all computerised and on the same database screens."



Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 187046 05/06 AM4298 335869

Printed on Paper containing 75% post consumer waste and 25% ECF pulp.

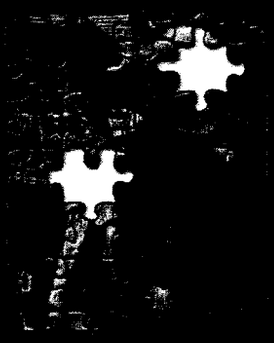
[redacted]



Publications Line
t: 08453 091 091
f: 0870 600 8181

Helpline
t: 01625 545745
f: 01625 524510

e: mail@ico.gsi.gov.uk
w: ico.gov.uk



May 2006

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

ICO/WPP/0506/3K

Information Commissioner's Office

[redacted]

Published by TSO (The Stationery Office) and available from:

Online
www.tso.co.uk/bookshop

Mail, Telephone, Fax and E-mail

TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-call 0845 7 023474
Fax orders: 0870 5533
E-mail: book.orders@tso.co.uk
Textphone 0870 240 3701

TSO Shops

123 Kingsway, London WC2B 6PQ
020 7242 6393 Fax 020 7242 6394

68-69 Bull Street, Birmingham B4 6AD
0121 236 9696 Fax 0121 236 9699

9-21 Princess Street, Manchester M60 8AS
0161 834 7201 Fax 0161 833 0634

16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401

18-19 High Street, Cardiff CF10 1PT
029 2039 5548 Fax 029 2038 4347

71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

TSO Accredited Agents

(see Yellow Pages)

and through good booksellers

ISBN 0-10-293767-2

9 780102 937671

[redacted]